report to be received from the State Government, the project shall be further considered.

(c) Question does not arise.

Power generation from nuclear sources

2480. SHRI DIPANKAR MUKHERJEE: Will the PRIME MINISTER be pleased to state:

(a) the target of power generation from nuclear sources during the Eighth Five Year Plan;

(b) the shortfall in the target and the reasons therefor; and

(c) the target of nuclear power generation during the Ninth Plan?

THE MINISTER OF STATE IN THE MINISTRY OF EXTERNAL AFAIRS (SHRIMATI VASUNDHARA RAJE): (a) The target for power generation from nuclear sources during the Eighth Five Year Plan was 37070 MUs.

(b) The actual generation of nuclear power during the Eighth Plan was 34844 MUs. The main reason for the short fall in power generation was due to turbo-generator blade failure and fire incident at Narora Atomic Power Station Unit-1 (NAPS-1) consequent upon which all the turbo-generators supplied by the Bharat Heavy Electricals Limited at all the stations had to be inspected, contributing to the reductions in generation during the period.

(c) The updated target of nuclear power generation during the Ninth Plan is estimated as 51854 MUs.

Leakage of sensitive information from BARC Computer

2481. SHRI JANARDHANA POOJARY:
SHRI SOLIPETA RAMACHANDRA REDDY:

Will the PRIME MINISTER be pleased to state:

(a) whether Government's attention has been drawn to a newsitem that appeared in the Sunday Times, dated 7th June, 1998 under the caption "Did hackers pilfer data from BARC site";

(b) if so, the details of the incident; and

(c) the steps Government have taken to check such incidents in future?

THE MINISTER OF STATE IN THE MINISTRY OF EXTERNAL AFFAIRS (SHRIMATI VASUNDHARA RAJE): (a) Yes, Sir.

(b) During the recent incident of breaking into the e-mail network, the hackers could access only some of the e-mail messages stored on the e-mail computers and could not get access to any information whatsoever stored on the other computers at BARC as there was no physical connection between e-mail network and the other computers. BARC has been following multiple level of security measures for safeguarding information stored on the computers. The computer systems for processing highly sensitive information are totally isolated, without any network or remote terminal connection and carried out in stand-alone environment with access to very limited users. There is no possibility of accessing these computers from outside BARC either through a network connection or dial-up telephone line.

(c) After the recent incident of unauthorised access to the e-mail computers at BARC, a committee was set up to look into the e-mail messages stored on these computers at the time of hacking. The committee, after scanning through all the messages confirmed that these messages did not contain any sensitive information. The technical contents appearing in these messages are regarding basic research results which would any way be published openly in scientific journals. Additional hardware and software protection measures are being implemented to further strengthen the security on e-mail computers and reduce the chance of unauthorised access to even public domain information available on the e-mail computers not only at BARC but also at all DAE units.